National Security
Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CAMPUS WIRELESS LAN v2.0
COMPLIANCE CHECKLIST

Campus WLAN Capability Package

Version 2.0

Campus WLAN Capability Package

March 18, 2016

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

The CSfC Campus WLAN CP meets the demand for Campus WLAN solutions using CNSSP 15 algorithms. These algorithms are used to protect classified data using layers of COTS products.

Table 1. IPSec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature) (Threshold – Unclassified Only)	RSA 3072	FIPS PUB 186-4
Authentication (Digital Signature) (Objective) (Threshold – All Classified NSS)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or DH 3072	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Top Secret	

Table 2. WPA2 Encryption and EAP-TLS (Approved Algorithms)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-128-CCMP (Threshold) AES-256-GCMP (Objective)	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
EAP-TLS Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (Threshold) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Objective)	IETF RFC 5216 IETF RFC 5246

2 REQUIREMENTS OVERVIEW

2.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist in this CP. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases

where this is not feasible solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional' in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold / Objective" column indicates that the Threshold equals the Objective (T=O).

Requirements that are listed as Objective in this CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this CP.

2.2 Requirements Designators

Each requirement defined in this CP has a unique identifier consisting of the prefix "WLAN," a digraph that groups related requirements together (e.g. "KM"), and a sequence number (e.g. 11).

Table 33 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

Table 3. Requirement Digraph

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 3	Table 44
SR	Overall Solution Requirements	Section 4.1	Table 55
EU	End User Device Requirements	Section 4.2	Table 66
WC	WLAN Client Configuration Requirements	Section 4.3	Table 77
WL	Wireless Link Requirements	Section 4.3	Table 88
CR	Configuration Requirements for VPN Components	Section 4.4	Table 99
WS	WLAN Access System Configuration Requirements	Section 4.5	Table 100
IA	Wireless Infrastructure Authentication Requirements	Section 4.5	Table 111
AA	Wireless Authentication and Authorization Requirements	Section 4.5	Table 122
WA	Wireless Authentication Server to WLAN Client Requirements	Section 4.5	Table 133
PF	Port Filtering Requirements for Solution Components	Section 4.6	Table 144
PR	End User Device (EUD) Provisioning Requirements	Section 4.7	Table 155
WI	Wireless Intrusion Detection Configuration Requirements	Section 4.8	Table 166
CM	Configuration Change Detection Requirements	Section 4.9	Table 177
DM	Device Management Requirements	Section 4.10	Table 1818

Digraph	Description	Section	Table
MR	Continuous Monitoring Requirements	Section 4.11	Table 1919
AU	Auditing Requirements	Section 4.12	Table 200
KM	Key Management Requirements	Section 4.134.13	Table 211 Table 222 Table 23 Table 24
FW	Gray Firewall Requirements	Section 4.144.14	Table 255
GD	Requirements for the Use and Handling of Solutions	Section 5.1	Table 266
RP	Incident Reporting Requirements	Section 5.2	Table 277
GD	Role-Based Personnel Requirements	Section 6	Table 2828
TR	Test Requirements	Section 7.1	Table 2929

3 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 4. Production Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-1	The product used for the VPN Gateway(s) shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O		
WLAN-PS-2	The products used for any WLAN Access System shall be chosen from the list of WLAN Access Systems on the CSfC Components List.	T=O		
WLAN-PS-3	The products used for any WLAN Client shall be chosen from the list of Mobile Platforms on the CSfC Components List. All validated Mobile Platform components include validated WLAN Client implementations.	T=O		
WLAN-PS-4	Products used for Mobile Platform EUDs shall be chosen from the list of Mobile Platforms on the CSfC Components List.	T=O		
WLAN-PS-5	The products used for the Inner VPN Client shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	T=O		
WLAN-PS-6	Intrusion Prevention Systems (IPS) shall be chosen from the list of IPS on the CSfC Components List.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-7	Products used for the Gray firewall shall be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	T=O		
WLAN-PS-8	Products used for the Authentication Server shall be chosen from the list of Authentication Servers on the CSfC Components List.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-9	The Inner VPN Gateway and the WLAN Access System shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. Differences between Service Packs (SP) and version numbers for a particular vendor's OS do not provide adequate diversity	T=O		
WLAN-PS-10	The WLAN Access System, Gray Firewall, Inner VPN Gateway shall use physically separate components, such that no component is used for more than one function.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-11	The Outer and Inner CAs shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. or Utilize a Enterprise PKI approved by the AO.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-12	The EUD's VPN Client and WLAN Client shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-13	The cryptographic libraries used by the WLAN Access System and the Inner VPN Gateway shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	Optional	
WLAN-PS-14	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 SCRM for additional guidance).	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PS-15	Components shall be configured to use the NIAP-certified evaluated configuration.	T=O		

4 CONFIGURATION REQUIREMENTS

Once the products for the solution are selected, the next Step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the WLAN solution.

4.1 OVERALL SOLUTION REQUIREMENTS

Table 5. Overall Solution Requirements (SR)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-SR-1	Default accounts, passwords, community strings and other default access control mechanisms for all Campus WLAN components shall be changed or removed.	T=O		
WLAN-SR-2	The time of day on the VPN Gateway shall be synchronized to a time source located in the Red network.	T=O		
WLAN-SR-3	The time of day on the WLAN Authentication Server, the WLAN Controller and Gray network Components shall be synchronized to a time source located in the Gray Management network.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-SR-4	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O		
WLAN-SR-5	Solution Components shall receive virus signature updates as required by the local agency policy and the AO.	T=O		
WLAN-SR-6	The only approved physical paths leaving the Red network shall be through a WLAN solution in accordance with this CP or via an AO-approved solution for protecting data in transit.[1]	T=O		

[1] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) product. In particular, it is acceptable for a given site to have both an egress path via an NSA-certified product and an egress path via a CSfC Solution conforming to a CP.

4.2 END USER DEVICES REQUIREMENTS

Table 6. End User Device (EU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-1	The EUD shall restrict configuration (Service Set Identifier (SSID) and authentication mechanism) of authorized WLANs to authorized administrators.	T=O		
WLAN-EU-2	The EUD shall be configured with separate authentication and privileges for administrator and user roles.	T=O		
WLAN-EU-3	The EUD shall be loaded with only AO-approved software.	T=O		
WLAN-EU-4	The EUD shall restrict installation and removal of software to authorized administrators.	T=O		
WLAN-EU-5	The EUD shall require a user to log in prior to granting access to any EUD functionality.	T=O		
WLAN-EU-6	The EUD shall be configured to limit the number of incorrect logins per an AO-approved period of time either by erasing the configuration and data stored on the device or by prohibiting login attempts for a AO-approved period of time.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-7	Rekeying of an EUD's certificates and associated private keys shall be done through re-provisioning prior to expiration of keys.	T	WLAN-EU-8	
WLAN-EU-8	Rekeying of an EUD's certificates and associated private keys shall be done over the WLAN solution network prior to expiration of keys.	O	WLAN-EU-7	
WLAN-EU-9	An EUD shall be deauthorized from the network and submitted for Forensic Analysis if suspected of being compromised.	T=O		
WLAN-EU-10	An EUD should be destroyed only if it has been determined to be compromised through Forensic Analysis.	T=O		
WLAN-EU-11	Users of EUDs shall successfully authenticate themselves to the services they access on their respective Red network using an AO-approved method.	T=O		
WLAN-EU-12	Red network services shall not transmit any classified data to EUDs until user authentication succeeds.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-13	The EUD shall lock the screen and require user re-authentication after an AO-approved period of inactivity.	T=O		
WLAN-EU-14	All EUD Users shall sign an organization-defined user agreement before being authorized to use an EUD.	T=O		
WLAN-EU-15	All EUD Users shall receive an organization-developed training course for operating an EUD prior to use.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-16	At a minimum, the organization-defined user agreement shall include each of the following: Consent to monitoring Operations Security (OPSEC) guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when, where, and under what conditions the EUD may be used • Responsibility for reporting security incidents • Verification of IA Training • Verification of appropriate clearance Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-17	EUDs shall be dedicated for use solely in the WLAN solution, and not used to access any resources on networks other than the Red network it communicates with through the two layers of encryption.	T=O		
WLAN-EU-18	The EUD shall disable all transmitted Global Positioning System (GPS) and location services except Enhanced 9-1-1 (E911) or those authorized by the AO.	T=O		
WLAN-EU-19	The EUD shall have all cellular access disabled.	T=O		
WLAN-EU-20	The EUD shall have all network and wireless interfaces disabled except for 802.11.	T=O		
WLAN-EU-21	The EUD shall have all cellular services disabled.	O	Optional	
WLAN-EU-22	All EUDs shall have their certificates revoked and resident image removed prior to disposal.	T=O		
WLAN-EU-23	Passwords for user-to-device authentication shall be a minimum of 4 alpha-numeric case sensitive characters.	T=O		
WLAN-EU-24	The native platform DAR protection shall be enabled[2].	T=O		

[2] If the WLAN Solution is implemented in conjunction with a NSA approved DAR Solution, then all applicable DAR CP requirements must also be implemented.

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-25	*Withdrawn*			
WLAN-EU-26	*Withdrawn*			
WLAN-EU-27	The EUD maximum password lifetime shall be less than 181 days.	T=O		
WLAN-EU-28	The EUD screen shall lock after an AO approved period of inactivity.	T=O		
WLAN-EU-29	The EUD shall perform a wipe of all protected data after 10 or more authentication failures.	T=O		
WLAN-EU-30	During provisioning, all unnecessary keys shall be destroyed from the EUD secure key storage.	T=O		
WLAN-EU-31	During provisioning, all unnecessary X.509 certificates shall be removed from the EUD Trust Anchor Database.	T=O		
WLAN-EU-32	All display notifications shall be disabled while in a locked state.	O	Optional	
WLAN-EU-33	USB mass storage mode shall be disabled on the EUDs.	O	Optional	
WLAN-EU-34	USB data transfer shall be disabled on the EUDs.	O	Optional	
WLAN-EU-35	Prior to installing new applications, the application digital signature shall be verified.	T=O		
WLAN-EU-36	The EUD shall be configured to only permit connections to whitelisted SSIDs.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-EU-37	The EUD shall be configured to only permit connection to SSIDs signed by the Outer CA.	T=O		
WLAN-EU-38	The EUD shall only display whitelisted SSIDs to the user.	T=O		
WLAN-EU-39	The EUD shall only permit the execution of Applications on a whitelist.	O	Optional	
WLAN-EU-40	The management and control of the EUD connection to the WLAN System shall be isolated from other EUD functions	O	Optional	

4.3 CONFIGURATION REQUIREMENTS FOR THE WLAN CLIENT

Table 7. WLAN Client (WC) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WC-1	The WLAN Client tunnel shall be established at EUD start-up.	T=O		
WLAN-WC-2	The WLAN Client shall authenticate the identity of the WLAN Authentication Server by verifying that the WLAN Authentication Server's certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WC-3	The WLAN Client shall be configured to authenticate only specific servers through setting the client to accept only a WLAN Authentication Server certificate that contains a particular Distinguished Name or Subject Alternate Name (i.e., the client looks for the specified server name in the certificate during verification).	T=O		
WLAN-WC-4	A unique device certificate shall be loaded into the WLAN Client along with the corresponding CA (signing) certificate.	T=O		
WLAN-WC-5	The device certificate shall be used for WLAN Client authentication during EAP-TLS.	T=O		
WLAN-WC-6	The WLAN Client shall provide the user with advance warning that the WLAN Client's device certificate is due to expire.	T=O		
WLAN-WC-7	The WLAN Client shall negotiate new session keys with the WLAN Access System at least once per hour.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WC-8	The WLAN Client shall be prevented from using ad hoc mode (client-to-client connections).	T=O		
WLAN-WC-9	The WLAN Client shall be prevented from using network bridging.	T=O		
WLAN-WC-10	The WLAN Client shall only associate with authorized Access Points based on attributes such as SSID or Whitelist and enforce based on the Certificate presented by the Authentication Server during mutual authentication.	T=O		
WLAN-WC-11	The WLAN Client shall verify that the WLAN Authentication Server X.509v3 certificate contains the TLS Web Server Authentication Object Identifier (OID) (id-kp-serverAuth 1.3.6.1.5.5.7.3.1) in the Extended Key Usage extension.	T=O		
WLAN-WC-12	The device certificate for the WLAN Client shall contain an extendedKeyUsage field indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WC-13	The WLAN Client shall be managed from the Gray Management Network accessible via the Campus WLAN.	T=O		

Table 8. Wireless Link (WL) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WL-1	The WLAN Client and the WLAN Access System shall use protocols and algorithms selected from table 2 that are approved to protect the highest classification level of the Red Network data.	T=O		
WLAN-WL-2	The WLAN Client and the WLAN Access System shall operate in WPA2-Enterprise mode.	T=O		
WLAN-WL-3	The WLAN Client and the WLAN Access System shall use integrity algorithms that implements NIST AES Key Wrap with HMAC-SHA-384-128 as specified in Section 11 of IEEE 802.11-2012.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WL-4	If WPA2 terminates on APs then all data between the Access Point(s) and Wireless controller shall be encrypted using IPsec, SSHv2, TLS, or TLS/HTTPS .	T=O		

4.4 CONFIGURATION REQUIREMENTS FOR VPN COMPONENTS AND VPN CLIENT

Table 9. Configuration Requirements (CR) for VPN Components

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CR-1	The VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 1 that are approved to protect the highest classification level of the Red Network data.	T=O		
WLAN-CR-2	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System and VPN Gateway , shall not be used for establishing Security Associations (SAs).	T	WLAN-CR-3	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CR-3	Default, self-signed, or proprietary device certificates, which are frequently preinstalled by the vendor, for any WLAN Access System and Inner VPN , shall be removed.	O	WLAN-CR-2	
WLAN-CR-4	All IPsec connections shall use IETF standards compliant IKE implementations (RFC 5996 or RFC 2409).	T=O		
WLAN-CR-5	All WLAN Components and Inner VPN Gateways shall use Cipher Block Chaining for IKE encryption.	T=O		
WLAN-CR-6	All WLAN Components and VPN Gateway shall use Cipher Block Chaining for ESP encryption with a Hash-based Message Authentication Code (HMAC) for integrity.	T	WLAN-CR-7	
WLAN-CR-7	All WLAN Components and VPN Gateway shall use Galois Counter Mode for ESP encryption.	O	WLAN-CR-6	
WLAN-CR-8	All WLAN Components and VPN Gateway shall set the IKE SA lifetime to at most 24 hours.	T=O		
WLAN-CR-9	All WLAN Components and VPN Gateway shall set the ESP SA lifetime to at most 8 hours.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CR-10	Each VPN Client shall use a unique private key for authenticating to the VPN Gateway.	T=O		
WLAN-CR-11	The VPN Client shall provide the user with advance warning that the VPN client certificate is due to expire.	T=O		
WLAN-CR-12	The VPN Client shall be configured to prohibit split tunneling.	T=O		
WLAN-CR-13	A unique device certificate shall be loaded into the VPN Client along with the corresponding CA (signing) Certificate	T=O		
WLAN-CR-14	The device certificate shall be used for VPN Client authentication during IPsec.	T=O		

4.5 Configuration Requirements for the WLAN Access System

The WLAN Access System is involved in establishing two encrypted channels. Once WLAN Authentication Server passes the PMK to the WLAN Access System, the WLAN Access System establishes an encrypted channel with the WLAN Client for passing data. The WLAN Access System acts as a pass-through for the initial authentication exchange between the WLAN Client and the WLAN Authentication Server during which the PMK is securely negotiated.

Table 10. WLAN Access System (WS) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WS-1	The WLAN Access System shall act as an EAP-TLS pass-through between the WLAN Client and WLAN Authentication Server for authentication and key establishment.	T=O		
WLAN-WS-2	The WLAN Access System shall negotiate new session keys with the WLAN Clients at least once per hour.	T=O		
WLAN-WS-3	Authentication performed by the WLAN Access System shall include a check that device certificates are authorized. This check may use a CRL, OCSP, or Whitelist.	T=O		
WLAN-WS-4	A unique device certificate shall be loaded into the Authentication Server along with the corresponding CA (signing) certificate.	T=O		
WLAN-WS-5	When supporting multiple enclaves, the WLAN Access System shall assign a firewall ACL to EUDs based on the attribute information provided by the Authentication Server.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WS-6	When supporting multiple enclaves, the WLAN Access System shall route EUD traffic over the appropriate interface based on attribute information provided by the Authentication Server.	T=O		
WLAN-WS-7	When supporting multiple enclaves, the WLAN Access System shall utilize unique physical internal interfaces for each enclave of the solution (e.g. VLAN Trunking of multiple enclaves is not permitted).	T=O		

Table 11. Wireless Infrastructure Authentication (IA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-IA-1	The WLAN Access System and the WLAN authentication server shall be physically co-located in the same rack and directly connected to each other.	T	WLAN-IA-2	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-IA-2	Communications between the WLAN Access System and the WLAN Authentication Server shall be established with either an IPsec tunnel (using either IKEv1 orIKEv2) or TLS/RADsec connection.	O	WLAN-IA-1	
WLAN-IA-3	The IKE exchange and IPsec tunnel between the WLAN Access System and the WLAN Authentication Server shall use protocols and algorithms selected from the Algorithm Suite in Table 11.	T=O		
WLAN-IA-4	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server shall be ESP using Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with a SHA-based HMAC for integrity .	T	WLAN-IA-5	
WLAN-IA-5	The ESP SA tunnel between the WLAN Access System and the WLAN Authentication Server shall be ESP use AES in Galois Counter Mode (GCM) mode.	O	WLAN-IA-4	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-IA-6	The lifetime of the IKE SA between the WLAN Access System and the WLAN Authentication Server shall be set to 24 hours.	T=O		
WLAN-IA-7	The lifetime of the ESP SA between the WLAN Access System and the WLAN Authentication Server shall be set to 8 hours or less.	T=O		
WLAN-IA-8	The WLAN Access System and the WLAN Authentication Server shall authenticate one another using X.509 version 3 certificates.	O	WLAN-IA-9	
WLAN-IA-9	The WLAN Access System and the WLAN Authentication Server shall authenticate one another using pre-shared keys.	T	WLAN-IA-8	
WLAN-IA-10	Composition rules for a pre-shared key between the WLAN Access System and the WLAN Authentication Server shall be set by the Security Administrator.	T=O		
WLAN-IA-11	The entropy of a pre-shared key between the WLAN Access System and the WLAN Authentication Server shall be a minimum of 256 bits.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-IA-12	The IKE exchange between the WLAN Access System and the WLAN Authentication Server shall use algorithms selected from Table 1.	T=O		

Table 12. Wireless Authentication and Authorization (AA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AA-1	The WLAN Authentication Server and WLAN Client shall perform mutual authentication using EAP-TLS with device certificates.	T=O		
WLAN-AA-2	The WLAN Client and the WLAN Authentication Server shall use the AES key size and mode for WPA2 Enterprise from the Threshold Section of Table 2.	T	WLAN-AA-3	
WLAN-AA-3	The WLAN Client and the WLAN Authentication Server shall use the AES key size and mode for WPA2 Enterprise from the Objective Section of Table 2.	O	WLAN-AA-2	
WLAN-AA-4	The WLAN Client and WLAN Authentication Server shall use the EAP-TLS Ciphersuite from the Threshold section of Table 2.	T	WLAN-AA-5	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AA-5	The WLAN Client and WLAN Authentication Servier shall use the EAP-TLS Ciphersuite from the Objective section of Table 2.	O	WLAN-AA-4	

Table 13. Wireless Authentication Server (WA) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WA-1	The WLAN Authentication Server (AS) shall use the most current CRL to check revocation status of the WLAN Client Certificate. If CRL does not exist, is invalid or has expired, authentication of the EUD will fail.	T=O		
WLAN-WA-2	The device certificate for the WLAN Authentication Server shall contain an extendedKeyUsage certificate extension indicating support for Server Authentication (Object Identifier (OID) 1.3.6.1.5.5.7.3.1).	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WA-3	The WLAN Authentication Server shall only successfully authenticate a WLAN Client if the WLAN Client's certificate contains an extendedKeyUsage certificate extension indicating support for Client Authentication (OID 1.3.6.1.5.5.7.3.2).	T=O		
WLAN-WA-4	The WLAN AS shall use the Distinguished Name or the Subject Alternate Name contained in the WLAN Client's certificate to authenticate the identity of the WLAN Client.	T=O		
WLAN-WA-5	The WLAN Authentication Server shall verify that the WLAN Client's certificate is not expired.	T=O		
WLAN-WA-6	The WLAN AS shall ensure that the WLAN Client's certificate chain is rooted by the WLAN trusted root Certificate Authority.	T=O		
WLAN-WA-7	*Withdrawn*			

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WA-8	The WLAN Authentication Server shall authenticate the identity of the WLAN Client by verifying that the WLAN Client's certificate is not revoked.	T=O		
WLAN-WA-9	When supporting multiple enclaves, the AS shall verify that the Common Name presented by the EUD certificate is included on a whitelist tied to an enclave.	T	WLAN-WA-10	
WLAN-WA-10	When supporting multiple enclaves, the AS shall verify that the certificate presented includes information in the Distinguished Name or Policy OIDs that ties the device to a single enclave.	O	WLAN-WA-9	
WLAN-WA-11	When supporting multiple enclaves, the AS shall provide attribute information on the appropriate enclave for the EUD to the Wireless Access System.	T=O		
WLAN-WA-12	The AS shall log all successful authentication attempts.	T=O		
WLAN-WA-13	The AS shall log all failed authentication attempts.	T=O		

4.6 PORT FILTERING REQUIREMENTS

Port Filtering is composed of a component configured with Access Control Lists (ACLs). The system ensures that the traffic flowing to and from each component on the network is appropriate for the functionality of the component within the Campus WLAN solution.

Table 14. Port Filtering (PF) Requirements for Solution Components

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PF-1	All Components within the Solution shall have all network interfaces restricted to the fewest address ranges, ports, and protocols possible.	T=O		
WLAN-PF-2	All Components within the Solution shall have all unused network interfaces disabled.	T=O		
WLAN-PF-3	For all interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only EAP-TLS, IKE, IPsec, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked.	T=O		
WLAN-PF-4	Any service or feature that allows an EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	T	WLAN-PF-5	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PF-5	Any service or feature that allows an EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	O	WLAN-PF-4	
WLAN-PF-6	The WLAN Access System shall block all data ports and IP addresses on their Gray Management network interface that are not necessary for the management of the WLAN Access System.	T=O		
WLAN-PF-7	Interfaces of the WLAN Access System shall be based on known MAC addresses of EUDs to further protect against unknown WLAN Clients.	T=O		
WLAN-PF-8	Traffic filtering rules on the EUD shall be applied based on known VPN Gateway addresses or address range to further protect against unknown IPsec traffic.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PF-9	The internal interface of the Inner VPN Gateway shall prohibit all management plane traffic (e.g. SSH, Remote Desktop Protocol (RDP), Telnet) originating from EUDs destined for the Red Network.	T=O		
WLAN-PF-10	The internal interface of the Inner VPN Gateway shall prohibit traffic destined for the Red Management Network (e.g. Red Management Network IP addresses) originating from End User Devices.	T=O		

4.7 End User Device (EUD) Provisioning Requirements

Table 15. EUD Provisioning Requirements (PR)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PR-1	A Provisioning WLAN using WPA2-PSK authentication and encryption shall be established on the Red network to support wireless provisioning of EUDs.	T		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PR-2	The Provisioning WLAN on the Gray Management Network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T		
WLAN-PR-3	The Provisioning WLAN on the Red network shall be contained within a shielded enclosure that provides 100 dB of attenuation across the frequency range from 2 to 6 GHz.	T		
WLAN-PR-4	EUDs shall be provisioned over the Provisioning WLANs.	T	WLAN-PR-5	
WLAN-PR-5	EUDs shall be provisioned over wired connections.	O	WLAN-PR-4	
WLAN-PR-6	When a EUD has been successfully provisioned, its identity (ITU-T X.509v3 Distinguished Name or Subject Alternate Name) shall be recorded in authorization databases accessible to the WLAN Authentication Server and VPN Gateway.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-PR-7	EUDs shall be provisioned to be disabled by having their certificates revoked.	T=O		
WLAN-PR-8	The EUD shall be loaded with an authorized software build during provisioning.	T=O		
WLAN-PR-9	The EUD shall be loaded with WLAN and VPN configuration profiles during provisioning.	T=O		
WLAN-PR-10	Strong passwords for the EUD shall be used to comply with the requirements of the policy established by the AO.	T=O		
WLAN-PR-11	Services not authorized by the AO shall be disabled during the provisioning of the EUD.	T=O		

4.8 Configuration Requirements for Wireless Intrusion Detection System (WIDS)

Table 16. Wireless IDS (WI) Configuration Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-1	The WIDS shall use a whitelist of all authorized wireless network devices (i.e. Access points and EUDs) and allow for administrator modifications.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-2	The WIDS shall detect access points which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O		
WLAN-WI-3	The WIDS shall detect EUDs which are not on the whitelist, but are within the coverage area of the WIDS sensors.	T=O		
WLAN-WI-4	The WIDS shall allow for administrator-defined rogue AP detection classification rules.	T=O		
WLAN-WI-5	The WIDS shall detect if a rogue AP is connected via wire to the network.	O	Optional	
WLAN-WI-6	The WIDS shall distinguish between the mere presence of unauthorized wireless hardware within the coverage area of the WIDS sensors and an attempt to use that hardware to gain access to the wireless network.	T=O		
WLAN-WI-7	All communication between WIDS components shall be done via a secure connection (using SSHv2, IPSec, TLS, or TLS/HTTPS).	O	Optional	
WLAN-WI-8	The WIDS shall geographically locate all wireless hardware operating in the coverage area of the WIDS sensors.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-9	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between unauthorized EUDs and authorized APs.	T=O		
WLAN-WI-10	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between unauthorized APs and authorized EUDs.	T=O		
WLAN-WI-11	The WIDS shall be configured to monitor all 802.11 frame types and subtypes between authorized APs and authorized EUDs.	T=O		
WLAN-WI-12	The WIDS shall allow for capturing the raw frames that triggered an alert as well as options on how long to continue capturing.	O	Optional	
WLAN-WI-13	The WIDS shall monitor and analyze traffic from all 802.11 channels within the 2.4Ghz and 4.9/5.0Ghz bands including those outside regulatory domain.	T=O		
WLAN-WI-14	The WIDS shall monitor and analyze traffic from all 802.11 channels within the 3.6Ghz and 60Ghz bands.	O	Optional	
WLAN-WI-15	The WIDS shall detect the use of unauthorized wireless channels by whitelisted devices.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-16	The WIDS shall determine which SSIDs are permitted on the network based on whitelisted APs or have the ability to be configured with a list of permitted SSIDs.	T=O		
WLAN-WI-17	The WIDS shall detect whitelisted APs using SSIDs not permitted on the network (including hidden SSID).	T=O		
WLAN-WI-18	The WIDS shall detect and log unauthorized APs broadcasting the same SSID as a whitelisted AP.	T=O		
WLAN-WI-19	The WIDS shall detect whitelisted EUDs associating to SSIDs not permitted on the network (including hidden SSID).	T=O		
WLAN-WI-20	The WIDS shall be configured to detect whitelisted devices attempting to use unauthorized authentication methods.	T=O		
WLAN-WI-21	The WIDS shall detect whitelisted devices attempting to use unauthorized encryption schemes.	T=O		
WLAN-WI-22	The WIDS shall be configured to process 802.11 traffic up to the data rate that is supported by the equipment in the wireless network.	T=O		
WLAN-WI-23	The WIDS shall log the signal strength of hardware operating in the coverage area of the WIDS sensors.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-24	The WIDS shall detect and log when it receives 802.11 frames being sent with a transmit power above maximum transmit power levels according to country regulations.	T=O		
WLAN-WI-25	The WIDS should support user-defined and customizable attack signatures.	T=O		
WLAN-WI-26	The WIDS shall detect RF-based Denial-of-Service (DoS) attacks.	T=O		
WLAN-WI-27	The WIDS shall perform protocol anomaly analysis to detect violations of WLAN standards such as 802.11 and 802.1X.	T=O		
WLAN-WI-28	The WIDS shall detect and log deauthentication flooding.	T=O		
WLAN-WI-29	The WIDS shall detect and log disassociation flooding.	T=O		
WLAN-WI-30	The WIDS shall use anomaly-based detection, to detect, log, and generate an alert when the network's activity deviates from an established network baseline.	O	Optional	
WLAN-WI-31	The WIDS shall monitor bandwidth usage.	O	Optional	
WLAN-WI-32	The WIDS shall monitor number of users/wireless clients.	O	Optional	
WLAN-WI-33	The WIDS shall monitor times of usage.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-34	The WIDS shall track the connection status of each client (authorized or unauthorized) in real time including, but not limited to, whether the client is offline, associated, or authentication is pending.	T=O		
WLAN-WI-35	The WIDS shall detect and log illegal state transitions, such as a client device transmitting data frames through an AP to a network device before being associated and authenticated.	T=O		
WLAN-WI-36	The WIDS shall detect and log an event where an attacker spoofs the Media Access Control (MAC) address of an authorized client to attempt to connect to the legitimate network.	T=O		
WLAN-WI-37	The WIDS shall detect and log an event where two sensors in physically separate (non-overlapping) locations (such as different buildings) receive frames with the same MAC address at the same time.	T=O		
WLAN-WI-38	The WIDS shall detect and log an event where a whitelisted EUD's MAC address appears in multiple physically distant locations.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-39	The WIDS shall detect whitelisted EUDs establishing peer-to-peer connections with other whitelisted devices or unauthorized devices.	O	Optional	
WLAN-WI-40	The WIDS shall detect EUDs bridging two network interfaces (wired and wireless). If the wired interface is connected to the internal network and the wireless interface is connected to a Rogue AP, this can expose traffic from the internal network.	O	Optional	
WLAN-WI-41	The WIDS shall detect and log the presence of an 802.11 bridge.	T=O		
WLAN-WI-42	The WIDS shall detect and log the presence of a single device transmitting beacons looking for a bridge.	T=O		
WLAN-WI-43	The WIDS shall detect and log the presence of two or more devices transmitting bridge data frames.	T=O		
WLAN-WI-44	The WIDS shall provide the ability to remove or disable all WIDS components' non-secure communications paths used for management and event monitoring including HTTP, SNMPv1, File Transfer Protocol (FTP), and Telnet.	T=O		
WLAN-WI-45	The WIDS shall allow for alert notification filtering such as alert notification type, severity levels, and number of alerts to receive.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-WI-46	The WIDS alert notifications shall be descriptive to show the significance of alerts.	T=O		
WLAN-WI-47	The WIDS must support the ability to export event logs and reports into industry standard formats such as Comma Separated Values (CSV) and Common Log Format (CLF).	T=O		

4.9 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 17. Configuration Change Detection (CM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	T=O		
WLAN-CM-2	An automated process shall ensure that configuration changes are logged.	T=O		
WLAN-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-CM-4	All Solution components shall be configured with a monitoring service that detects all changes to configuration.	T=O		

4.10 Device Management Requirements

Only authorized Security Administrators will be allowed to administer the Components. The WLAN solution will be used as transport for the Secure Shell (SSH)v2, IPsec, or TLS data from the Administration Workstation to the Component.

Table 18. Device Management (DM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-DM-1	Administration Workstations shall be dedicated for the purposes given in the CP and shall be physically separated from workstations used to manage non-CSfC solutions.	T=O		
WLAN-DM-2	*Withdrawn*			
WLAN-DM-3	Antivirus software shall be running on all Administration Workstations.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-DM-4	All components shall be configured to restrict the IP address range for the network administration device to the smallest range possible.	T=O		
WLAN-DM-5	The Gray Management network shall not be directly connected to Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O		
WLAN-DM-6	All administration of solution components shall be performed from an Administration Workstation remotely using one of SSHv2, IPsec, or TLS 1.2 or later version; or by managing the solution components locally.	T=O		
WLAN-DM-7	Security Administrators shall authenticate to solution components before performing administrative functions.	T	WLAN-DM-8	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-DM-8	Security Administrators shall authenticate to solution components with Suite B-compliant certificates before performing administrative functions remotely.	O	WLAN-DM-7	
WLAN-DM-9	Security Administrators shall establish a security policy for EUDs per the implementing organization's local policy.	T=O		
WLAN-DM-10	EUDs shall generate logs and send to a central SIEM in the Red network.	O	Optional	
WLAN-DM-11	Security Administrators shall initiate certificate signing requests for solution components as part of their initial keying within the solution.	T=O		
WLAN-DM-12	Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-DM-13	The WLAN Access System and solution components within the Gray network shall forward log entries to a SIEM on the Gray Management network (or SIEM in the Red Network if using an AO approved one-way tap) within 10 minutes.	T=O		
WLAN-DM-14	All logs forwarded to a SIEM on the Gray Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	T	WLAN-DM-15	
WLAN-DM-15	All logs forwarded to a SIEM on a Red Management network shall be encrypted using SSHv2, IPsec, or TLS 1.1 or later.	O	WLAN-DM-14	
WLAN-DM-16	When managing Solution components over the Black network, the management traffic shall be encrypted with Suite B algorithms IAW Table 2.	T=O		

4.11 CONTINUOUS MONITORING REQUIREMENTS

Table 19. Continuous Monitoring (MR) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-MR-1	Traffic on the Gray and before the Red networks shall be monitored from an Intrusion Detection System (IDS).	T	WLAN-MR-2	
WLAN-MR-2	Traffic on the Gray and before Red networks shall be monitored from an Intrusion Prevention System (IPS).	O	WLAN-MR-1	
WLAN-MR-3	The WIDS shall encrypt and sign all alerts pushed to a remote system administrator.	O	WLAN-MR-4	
WLAN-MR-4	System administrators shall authenticate all alerts received by the WIDS.	T	WLAN-MR-3	
WLAN-MR-5	All event monitoring of the WIDS shall be remotely performed from the Gray Management Network through SSHv2, IPsec, or TLS.	T=O		
WLAN-MR-6	The IDS in the solution shall be configured to send alerts to the Security Administrator.	T	WLAN-MR-7	
WLAN-MR-7	The IPS in the solution shall be configured to block malicious traffic flows and alert the Security Administrator.	O	WLAN-MR-6	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-MR-8	The IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized destination IP addresses.	T	WLAN-MR-9	
WLAN-MR-9	The IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	WLAN-MR-8	
WLAN-MR-10	The IDS in the solution shall be configured with rules that generate alerts upon detection of any unauthorized source IP addresses.	T	WLAN-MR-11	
WLAN-MR-11	The IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	WLAN-MR-10	
WLAN-MR-12	A Network-based Intrusion Detection System (NIDS) shall be deployed on the Gray Management Network to monitor traffic arriving from or leaving to the WLAN Access System.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-MR-13	The NIDS shall report all matches to the attack signatures on the NIDS to both inbound and outbound traffic.	O	Optional	
WLAN-MR-14	The NIDS shall be regularly updated with attack signatures in accordance with local policy.	O	Optional	

4.12 AUDITING REQUIREMENTS

Table 20. Auditing (AU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AU-1	VPN Gateways shall log establishment of a VPN tunnel.	T=O		
WLAN-AU-2	VPN Gateways shall log termination of a VPN tunnel.	T=O		
WLAN-AU-3	VPN Clients shall log establishment of a VPN tunnel.	T=O		
WLAN-AU-4	VPN Clients shall log termination of a VPN tunnel.	T=O		
WLAN-AU-5	Solution components shall log all actions performed on the audit log (off-loading, deletion, etc.).	T=O		
WLAN-AU-6	Solution components shall log all actions involving identification and authentication.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AU-7	Solution components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	T=O		
WLAN-AU-8	Solution components shall log all actions performed by a user with super-user or administrator privileges.	T=O		
WLAN-AU-9	Solution components shall log escalation of user privileges.	T=O		
WLAN-AU-10	Solution components shall log generation, loading, and revocation of certificates.	T=O		
WLAN-AU-11	Solution components shall log changes to time.	T=O		
WLAN-AU-12	Each log entry shall record the date and time of the event.	T=O		
WLAN-AU-13	Each log entry shall include the identifier of the event.	T=O		
WLAN-AU-14	Each log entry shall record the type of event.	T=O		
WLAN-AU-15	Each log entry shall record the success or failure of the event to include failure code, when available.	T=O		
WLAN-AU-16	Each log entry shall record the subject identity.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AU-17	Each log entry shall record the source address for network-based events.	T=O		
WLAN-AU-18	Each log entry shall record the user and, for role-based events, role identity, where applicable.	T=O		
WLAN-AU-19	Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	O	Optional	
WLAN-AU-20	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated CRL to the Security Administrator.	O	Optional	
WLAN-AU-21	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same EUD device certificate.	O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-AU-22	The WIDS shall log when sensors fail to communicate.	T=O		
WLAN-AU-23	The EUD shall log all successful and unsuccessful logins.	O	Optional	
WLAN-AU-24	The EUD shall log all successful and unsuccessful logouts.	O	Optional	
WLAN-AU-25	The EUD shall audit installation and removal of software.	O	Optional	
WLAN-AU-26	The EUD shall audit attempts to change security-relevant configuration items.	O	Optional	
WLAN-AU-27	The EUD shall audit changes to security-relevant configuration items.	O	Optional	
WLAN-AU-28	The EUD shall audit signature verification and certificate validation.	O	Optional	
WLAN-AU-29	Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis.	T=O		

4.13 Key Management Requirements

4.13.1 General Requirements

Table 21. PKI General (KM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-1	User certificates and user private keys shall be classified to the level determined by the AO and compliant with CNSSI 4005.	T=O		
WLAN-KM-2	A locally-operated CA supporting the VPN Gateway shall be physically separate from a locally-supported CA supporting the Wireless Controller and Authentication Server.	T = O		
WLAN-KM-3	All public/private key pairs and certificates for the VPN Gateway and Wireless Controller and Authentication Server shall be used for authentication only.	T=O		
WLAN-KM-4	The Outer and Inner CAs shall each operate in compliance with Certificate Policy and Certification Practice Statement (CPS) that are formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	T=O		
WLAN-KM-5	The Gray and Inner CAs shall rekey infrastructure devices and EUDs prior to expiration of keys.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-6	Authentication certificates issued by the Gray and Inner CAs for the Solution shall be X.509 v3 certificates as defined in ITU-T Recommendation X.509.	T=O		
WLAN-KM-7	All device certificates issued by the Gray and Inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	T=O		
WLAN-KM-8	CAs shall run anti-virus software.	T=O		
WLAN-KM-9	CAs shall not escrow private keys.	T=O		
WLAN-KM-10	If multiple Red enclaves exist in the WLAN Solution and the Outer CA resides in the Red network, the Outer CA must reside in the Red network with the highest classification level.	T=O		
WLAN-KM-11	Outer CAs shall provide services through either the Gray or Red network.	T=O		
WLAN-KM-12	Inner CAs shall provide services through the Red Network.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-13	All certificates issued by the Outer and Inner CAs for the WLAN Solution shall be Non-Person Entity (NPE) certificates.	T=O		
WLAN-KM-14	Authentication certificate profiles for the Gray and Inner CAs for the WLAN Solution shall comply with IETF RFC 5280.	T=O		
WLAN-KM-15	The key sizes and algorithms for CA certificates and authentication certificates issued to Authentication Server, the VPN Gateway, and Administrative Device Components shall be as illustrated in Tables 1 and 2.	T=O		
WLAN-KM-16	Private keys associated with on-line, locally run Outer and Inner CAs shall be protected using Hardware Security Modules (HSMs) validated to at least FIPS 140-2 Level 2. "On-line" means the CA is always powered on and network-accessible.	T=O		

4.13.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 22. Certificate Issuance Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-17	Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification level of the MA solution network.	T=O		
WLAN-KM-18	Outer and Inner CAs shall use Public Key Cryptographic Standard PKCS#10 and PKCS#7 to issue authentication certificates to Outer WLAN Components, Inner VPN Components, and Gray and Red Management Services Components.	T	WLAN-KM-21	
WLAN-KM-19	Red and Gray Management Services shall use PKCS#12 for installing certificates/keys to EUDs.	T	WLAN-KM-20	
WLAN-KM-20	Red and Gray Management Services shall use PKCS#7 for installing certificates to EUDs.	O	WLAN-KM-19	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-21	Outer and Inner CAs shall use IETF RFC 7030 Enrollment over Secure Transport (EST) to issue authentication certificates to Outer WLAN Components, Inner VPN Components, and Gray and Red Management Services Components.	O	WLAN-KM-18	
WLAN-KM-22	Certificate signing requests Gray and Red Management Services Components shall be submitted to the CA in accordance with the CA's Certificate Policy and Certification Practices Statement (CPS).	T=O		
WLAN-KM-23	Outer and Inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	T=O		
WLAN-KM-24	Certificate Policies and CPSs for non-Enterprise, locally-run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: • Unique Distinguished Names (DNs) • Appropriate key usages • A registered policy Object Identifier (OID)	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-25	Outer and Inner CAs shall assert at least one CRL Distribution Point (CDP) Uniform Resource Locater (URL) in certificates issued to Solution Infrastructure VPN Gateway, Wireless controller and Authentication Server, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs.	T=O		
WLAN-KM-26	The key validity period for certificates issued by non-Enterprise, locally run CAs to WLAN EUDs shall not exceed 14 months.	T=O		
WLAN-KM-27	The key validity period for certificates issued by non-Enterprise, locally run CAs to WLAN Solution Infrastructure Components shall not exceed 36 months.	T=O		
WLAN-KM-28	Inner CAs shall only issue certificates to the VPN Gateway and Red Network Components of WLAN Solutions.	T=O		
WLAN-KM-29	Outer CAs shall only issue certificates to Wireless Controller, WLAN Clients and Authentication Server.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-30	The Outer CA shall issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage certificate extension.	O	Optional	
WLAN-KM-31	The Outer CA shall issue certificates to WLAN Clients that contain the Client Authentication OID (1.3.6.1.5.5.7.3.2) in the ExtendedKeyUsage certificate extension and in the extended KeyUsage certificate extension.	T=O		
WLAN-KM-32	The VPN Gateway shall only trust the Inner CA used for its network.	T=O		
WLAN-KM-33	WLAN Components shall only trust the Outer CA used within the solution.	T=O		

4.13.3 CERTIFICATE RENEW AND REKEY REQUIREMENTS

Table 23. Certificate Renew and Rekey Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-34	Certificate renewal or rekey shall occur prior to a certificate expiring.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-35	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	T=O		
WLAN-KM-36	Outer and Inner CAs shall issue renewed/ rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	T	WLAN-KM-37	
WLAN-KM-37	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using EST (RFC 7030).	O	WLAN-KM-36	

4.13.4 CERTIFICATE REVOCATION REQUIREMENTS

Table 24. Certificate Revocation Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-38	Outer and Inner CAs shall revoke a certificate issued to WLAN Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-39	Outer and Inner CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	T=O		
WLAN-KM-40	CRLs shall be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	T=O		
WLAN-KM-41	CRL profiles shall comply with IETF RFC 5280.	T=O		
WLAN-KM-42	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and Certification Practices Statement.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-43	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure revocation procedures address the following: • Response for a lost, stolen or compromised WLAN EUD • Removal of a revoked infrastructure device (i.e., VPN Gateway) from the network • Re-establishment of a WLAN Solution Component whose certificate was revoked • Revocation of certificates due to compromise of an WLAN EUD • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-44	Outer and Inner CAs shall make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	T=O		
WLAN-KM-45	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O		
WLAN-KM-46	Non-enterprise, locally run CAs shall publish new CRLs at least once every 28 days.	T=O		
WLAN-KM-47	Non-enterprise, locally run CAs shall publish a new CRL within one hour of a certificate being revoked.	T=O		
WLAN-KM-48	Solution Infrastructure Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	T=O		
WLAN-KM-49	Non-enterprise, locally run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-KM-50	The WLAN Solution shall provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray network that is compliant with IETF RFC 6960.	O	Optional	
WLAN-KM-51	Certificate revocation status messages delivered by an OCSP server shall be digitally signed and compliant with IETF RFC 6960.	O	Optional	

4.14 GRAY FIREWALL REQUIREMENTS (FW)

Table 25. Gray Firewall Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-FW-1	Gray Network Firewall shall permit IKE and IPsec traffic between the EUDs VPN Client and VPN Gateway protecting networks of the same classification level.	T=O		
WLAN-FW-2	Gray Network Firewall shall allow HTTP traffic between the Authentication Server and Gray CDP or OCSP responder.	T	WLAN-FW-3 and WLAN-FW-4	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-FW-3	Gray Network Firewall shall allow HTTP GET requests from the Authentication Server to the Gray CDP or OCSP responder for the URL of the CRL OCSP Response needed by the VPN Gateway, and block all other HTTP requests.	O	WLAN-FW-2	
WLAN-FW-4	Gray Network Firewall shall allow HTTP responses from the Gray CDP or OCSP responder to the Authentication Server that contain a well-formed CRL per IETF RFC 5280 or OCSP Response per RFC 6960, and block all other HTTP responses.	O	WLAN-FW-2	
WLAN-FW-5	Gray Network Firewall shall only accept management traffic on the physical ports connected to the Gray Management network.	T=O		
WLAN-FW-6	Gray Network Firewall shall only permit packets whose source and destination IP addresses match the external interfaces of the VPN Components that support Red networks of the same classification level.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-FW-7	Gray Network Firewall shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O		
WLAN-FW-8	Gray Network Firewall shall deny all traffic that is not explicitly allowed by requirements WLAN-FW-1, WLAN-FW-2, WLAN-FW-3, WLAN-FW-4, or WLAN-FW-5.	T=O		
WLAN-FW-9	Gray Network Firewall shall allow control plane traffic (NTP, DHCP, DNS).	T=O		

5 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

5.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS (GD)

The following requirements shall be followed regarding the use and handling of the solution.

Table 26. Requirements for the Use and Handling of Solutions

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-1	All Solution Infrastructure components shall be physically protected as classified devices, classified at the highest classification level of the Red network.	T=O		
WLAN-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the solution Infrastructure components.	T=O		
WLAN-GD-3	Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs.	T=O		
WLAN-GD-4	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O		
WLAN-GD-5	EUDs using a NSA-approved DAR solution shall be disposed of in accordance with the disposal requirements for the DAR solution.	T=O		
WLAN-GD-6	All EUDs shall have their certificates revoked prior to disposal.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-7	Users shall periodically inspect the physical attributes of EUDs for signs of tampering or other unauthorized changes.	T=O		
WLAN-GD-8	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	T=O		
WLAN-GD-9	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the CP.	T=O		
WLAN-GD-10	The AO will ensure that a compliance audit shall be conducted every year against the latest version of the WLAN CP as part annual solution re-registration process.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-11	Results of the compliance audit shall be provided to and reviewed by the AO.	T=O		
WLAN-GD-12	Customers interested in registering their solution against the WLAN CP shall register with NSA and receive approval prior to AO authorization to operate.	T=O		
WLAN-GD-13	The implementing organization shall complete and submit a WLAN CP requirements compliance matrix to their respective AO.	T=O		
WLAN-GD-14	Registration and re-registration against the WLAN CP shall include submission of WLAN CP registration forms and compliance matrix to NSA.	T=O		
WLAN-GD-15	When a new approved version of the WLAN CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months or by the next re-registration date (whichever is greater).	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-16	Solution implementation information, which was provided to NSA during solution registration, shall be updated annually as part annual solution re-registration process.	T=O		
WLAN-GD-17	Audit log data shall be maintained for a minimum of 1 year.	T=O		
WLAN-GD-18	The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	T=O		
WLAN-GD-19	Audit data shall be frequently off-loaded to a backup storage medium.	T=O		
WLAN-GD-20	A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-21	The implementing organization shall develop a continuity of operations plan for auditing capability, which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	T=O		
WLAN-GD-22	The implementing organization shall develop a continuity of operations plan for auditing capability, which includes a mechanism or method for off-loading audit log data for long- term storage.	T=O		
WLAN-GD-23	The implementing organization shall develop a continuity of operations plan for auditing capability, which includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O		
WLAN-GD-24	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-25	Strong passwords shall be used that comply with the requirements of the AO.	T=O		
WLAN-GD-26	Security critical patches shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	T=O		
WLAN-GD-27	Local policy shall dictate how the Security Administrator will install patches to solution components.	T=O		
WLAN-GD-28	Solution components shall comply with local TEMPEST policy.	T=O		
WLAN-GD-29	Software, settings, keys, and all other configuration data persistently stored on EUDs shall be handled as controlled unclassified information or higher classification.	T=O		
WLAN-GD-30	All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	T=O		

Additional WLAN-GD requirements can be found in Section 6.

5.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 27 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators, Certificate Authority Administrators (CAAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary, but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 27 only provides requirements directly related to the incident reporting process. See Section 4.11 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

Table 27. Incident Reporting Requirements (RP)

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-RP-1	Solution owners shall report confirmed incidents meeting the criteria in WLAN RP-3 through WLAN-RP-16 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Name of affected Network(s) • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	T=O		
WLAN-RP-3	Solution owners shall report a security failure in any of the CSfC solution components.	T=O		
WLAN-RP-4	Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC Solution.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-RP-5	For Gray network interfaces, solution owners shall report any malicious inbound and outbound traffic.	T=O		
WLAN-RP-6	Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O		
WLAN-RP-7	Solution owners shall report if a solution component sends traffic with an unauthorized destination address.	T=O		
WLAN-RP-8	Solution owners shall report any malicious configuration changes to the components.	T=O		
WLAN-RP-9	Solution owners shall report any unauthorized escalation of privileges to any of the CSfC solution components.	T=O		
WLAN-RP-10	Solution owners shall report if two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	T=O		
WLAN-RP-11	Solution owners shall report any evidence of malicious physical tampering with solution components.	T=O		
WLAN-RP-12	Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data.	T=O		
WLAN-RP-13	Solution owners shall report any significant degradation of services provided by the solution.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-RP-14	Solution owners shall report malicious discrepancies in the number of connections established the WLAN Access System.	T=O		
WLAN-RP-15	Solution owners shall report malicious discrepancies in the number of VPN connections established by the Inner VPN Gateway.	T=O		

6 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the WLAN solution. Security Administrator duties include, but are not limited to, the following:

1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the WLAN solution.

5) Ensuring that the implemented WLAN solution remains compliant with the latest version of this CP.

6) Provisioning and maintaining EUDs in accordance with this CP for implementations that include them.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include, but are not limited to, the following:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating the CRL.

3) Provisioning and maintaining EUD certificates in accordance with this CP for implementations that include them.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the WLAN solution. Auditor duties include, but are not limited to, the following:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to Outer and Inner administrative components.

Solution Integrator – In certain cases, an external integrator may be hired to implement a WLAN solution based on this CP. Solution Integrator duties may include, but are not limited to, the following:

1) Acquiring the products that compose the solution.

2) Configuring the WLAN solution in accordance with this CP.

3) Documenting, testing, and maintaining the solution.

4) Responding to incidents affecting the solution.

End User –An End User may operate an EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. Remote User duties include, but are not limited to the following:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.

2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in a WLAN Solution are as follows:

Table 28. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-31	The Security Administrator, CAAs, Auditor, EUD User, and Solution Integrators shall be cleared to the highest level of data protected by the Solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.	T=O		
WLAN-GD-32	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	T=O		
WLAN-GD-33	All Security Administrators, CAAs, EUD Users, and Auditors shall meet local Information Assurance (IA) training requirements.	T=O		
WLAN-GD-34	The CAA(s) for the Inner tunnel shall be different individuals from the CAA(s) for the Outer tunnel.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-35	Upon discovering an EUD is lost, stolen or altered, an EUD User shall immediately report the incident to their Security Administrator and Certificate Authority Administrator.	T=O		
WLAN-GD-36	Upon notification of a lost, stolen or altered EUD, the Certificate Authority Administrators shall revoke that EUD's certificates.	T=O		
WLAN-GD-37	The Security Administrator(s) for the Inner Encryption Endpoints and supporting components on Enterprise/Red networks shall be different individuals from the Security Administrator(s) for the Outer VPN Gateway and supporting components on Gray networks.	T=O		
WLAN-GD-38	Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	O	Optional	

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-GD-39	The Auditor shall review all logs specified in this CP at least once a week.	T=O		
WLAN-GD-40	Security Administrators shall initiate the certificate revocation process prior to disposal of any solution component.	T=O		
WLAN-GD-41	Auditing of the Outer and Inner CA operations shall be performed by individuals who were not involved in the development of the Certificate Policy and CPS, or integration of the WLAN solution.	T=O		

7 INFORMATION TO SUPPORT AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the WLAN solution..
- The customer has system certification and accreditation performed using the risk assessment information.
- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented in accordance with the CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use.

- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the WLAN CP, and the results shall be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the solution in the case of a compromise.
- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO will report incidents affecting the solution in accordance with Section 5.2.

The system AO maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO shall ensure that the solution remains properly configured with all required security updates implemented.

7.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a WLAN solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

Table 29. Test Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets this requirement)
WLAN-TR-1	The organization implementing the CP shall perform all tests listed in Section 16 of WLAN CP v2.0.	T=O		